

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

The property to be searched is as follows:

- a. Samsung Galaxy Z Fold cellular telephone, serial number RFCX50427RJ,
IMEI # 357502651744033;

The Device is currently located at the U.S. Probation Office for the Eastern District of Wisconsin evidence locker located at 517 E. Wisconsin Avenue, Room #001, Milwaukee, Wisconsin 53202.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 USC 2252 and 2252A, including:
 - a. Records containing child pornography or pertaining to the production, distribution, receipt, or possession of child pornography;
 - b. Records or information, photographs, videos, notes, documents, or correspondence, in any format or medium, concerning communications about child pornography or sexual activity with or sexual interest in minors;
2. All names, aliases, and numbers stored in the Device, including numbers associated with the Device, relating to the identities of those engaged in the production, possession, receipt, or distribution of child pornography.
3. Images or visual depictions of child pornography.
4. Records and information containing child erotica, including texts, images, and visual depictions of child erotica.
5. Any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to the violations.
6. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted by use of the computer or by other means for the purpose of committing the violations.
7. The list of all telephone calls made or received located in the memory of the Devices that provides information regarding the identities of and the methods and means of operation and communication by those engaged in the possession, receipt, or distribution of child pornography.
8. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning membership in online groups, clubs, or services that provide or make accessible child pornography.

9. Any and all information, records, documents, invoices, and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to the violations.

10. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Samsung Galaxy Z Fold cellular telephone, serial number RFCX50427RJ,
IMEI # 357502651744033, which is currently located at the U.S.
Probation evidence locker, Room 001, 517 East Wisconsin Avenue,
Milwaukee, WI, described on Attachment A.

Case No. 25-945M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the _____ Eastern _____ District of _____ Wisconsin _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

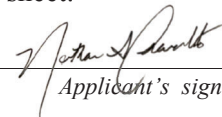
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Section 2252A(a)(5) (B) and (b)(2)	Possession of and access with intent to view child pornography

The application is based on these facts:

See Attached Affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



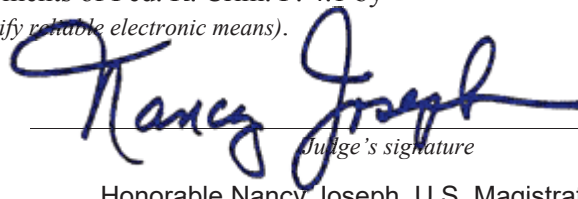
Applicant's signature

Nathan A. Cravatta, Special Agent - HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
 _____ telephone _____ (specify reliable electronic means).

Date: 5/29/2025



Judge's signature

City and state: Milwaukee, Wisconsin

Honorable Nancy Joseph, U.S. Magistrate Judge

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Nathan A. Cravatta, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – an electronic device – which is currently in the custody of the U.S. Probation Office for the Eastern District of Wisconsin, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI), an investigative branch of the United States Department of Homeland Security. I am a federal law enforcement officer authorized by the Secretary of Homeland Security to request the issuance of criminal complaints and search warrants. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have been employed as a Special Agent with HSI since May 2005. I am currently assigned to the Resident Agent in Charge Office in Milwaukee, Wisconsin.

3. My experience as an HSI agent has included the investigation of cases involving the use of computers and the Internet to commit violations of federal law involving child exploitation, including the production, transportation, receipt,

distribution, and possession of child pornography. I have received training and have gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications and the execution of searches and seizures involving computer crimes. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children which constituted violations of Title 18, United States Code, Sections 2251, 2252 and 2252A.devices

4. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, incorporated herein by reference as if fully set forth, are located in the Device for which authority is requested to search. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is a Samsung Galaxy Z Fold cellular telephone, serial number RFCX50427RJ, IMEI # 357502651744033 ("Device"),

6. The Device is currently located at the U.S. Probation Office for the Eastern District of Wisconsin evidence locker located at 517 E. Wisconsin Avenue, Room #001, Milwaukee, Wisconsin 53202. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this

investigation, in substantially the same state as they were when the Device first came into the possession of the U.S. Probation Office.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

8. The purpose of this application is to seize evidence of violations of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography).

PROBABLE CAUSE

Information Obtained from the U.S. Probation Office for the Eastern District of Wisconsin

9. On May 19, 2025, U.S. Probation Officer (USPO) Patricia Savasta provided information indicating on April 18, 2025, she was provided information indicating Grant RONDORF, who is on supervised release, was in the possession of an unauthorized cellular telephone. As a condition of his supervised release, RONDORF is not allowed to possess and/or use a computer or other electronic communications or data storage devices or media; unless approved by his probation officer.

10. On May 15, 2025, USPO Savasta conducted a home visit at the residence of RONDORF in West Bend, Wisconsin. He was directed to turn over the cellular telephone. RONDORF initially denied having a cellular telephone; however, he eventually admitted to having an unauthorized phone. RONDORF retrieved the Device from his bedroom dresser drawer and provided it to USPO Savasta. RONDORF

also provided the password for the Device. When questioned if there would be anything of interest on the Device, RONDORF responded, "there shouldn't be."

11. After returning to her office, USPO Savasta manually reviewed the files on Device. USPO observed several images of a male penis. Additionally, USPO Savasta observed an image of an adult penis positioned in front of a toddler's face. USPO Savasta terminated her review of the Device.

PRIOR CONVICTION FOR DISTRIBUTION OF CHILD PORNOGRAPHY

12. On November 21, 2012, a HSI special agent acting in an undercover capacity downloaded 125 files which depicted child sexual abuse material (CSAM) from a Giga Tribe Peer to Peer file sharing network user identified as "gruntt33." The Internet Protocol (IP) used to facilitate the distribution of these files resolved to a Charter Communications subscriber residing in Madison, Wisconsin.

13. On January 29, 2013, special agents with HSI Milwaukee executed a search warrant at this residence. Seized from the residence was a laptop computer later determined to contain 5,301 images and 509 videos which depicted CSAM. Also located was a thumb drive determined to contain thirty-seven images and thirty-nine videos which depicted CSAM. The files depicted infants and children up to the age of nine posing naked, or engaging in sexual activities with adults or other children.

14. Present during the execution of the search warrant was Grant RONDORF. During a consensual interview conducted with RONDORF, he admitted to being the

owner and user of the laptop computer and thumb drive. RONDORF also admitted to possessing the CSAM files located on both devices.

15. On May 13, 2013, RONDORF was indicted by a grand jury sitting in the Western District of Wisconsin for eight counts of distribution of child pornography in violation of 18 U.S.C. 2252 (a)(2) and two counts of accessing devices containing visual depictions of minors engaging in sexual activity that had been produced using materials which have been shipped and transported in interstate and foreign commerce in violation of 18 U.S.C. 2252 (a)(4)(B).

16. On October 8, 2013, RONDORF was sentenced to ninety-six months imprisonment followed by twenty years of supervised release for one count of Distribution of Child Pornography. He was released from prison on November 22, 2019.

17. On January 31, 2020, a Transfer of Jurisdiction order was approved by the U.S. District Court for the Eastern District of Wisconsin.

18. On June 30, 2023, RONDORF's supervised release was revoked by the Court for failing to comply with sex offender treatment, possessing an electronic device without the authorization of his probation officer, and failing to follow the instructions of his probation officer. The Court sentenced RONDORF to twenty-eight days in prison followed by one hundred ninety-two months of supervised release. He was released from prison on September 11, 2023.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning

System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- d. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static – that is, long-term – IP addresses, while other computers have dynamic – that is, frequently changed – IP addresses.
- e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social network.

20. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at [https:// www.samsung.com/us/smartphones/galaxy-z-fold6/](https://www.samsung.com/us/smartphones/galaxy-z-fold6/), I know that the Samsung Galaxy Z Fold cellular telephone have capabilities that allow them to serve all or some of the following functions: wireless telephone, a digital camera, GPS navigation device, and accessing / downloading information from the Internet. In my training and experience, examining data stored on devices of these types can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. As explained below, information stored within a cellular phone (cell phone) or tablet ("Devices") may provide crucial evidence of the "who, what, why, when, where, and how" of the conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored within the devices can indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search

warrant at a residence. For example, contacts lists, instant messaging logs, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the devices at a relevant time. Further, such stored electronic data can show how and when the devices and its related account were accessed or used. Such “timeline” information allows investigators to understand the chronological context of device access, use, and events relating to the crime under investigation. This “timeline” information may tend to either inculcate or exculpate the devices account owner. Additionally, information stored within a device may indicate the geographic location of the devices and user at a particular time (e.g., location integrated into an image or video sent via email or text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the devices owner’s state of mind as it relates to the offense under investigation. For example, information in the devices may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement). Unless this data is destroyed, by breaking the devices itself or by a program that deletes or over-writes the data contained within the device, such data will remain stored within the devices indefinitely.

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that

establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to obtain unauthorized access to a victim electronic device over the Internet the individual’s electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of

the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

26. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

ATTACHMENT A

The property to be searched is as follows:

- a. Samsung Galaxy Z Fold cellular telephone, serial number RFCX50427RJ,
IMEI # 357502651744033;

The Device is currently located at the U.S. Probation Office for the Eastern District of Wisconsin evidence locker located at 517 E. Wisconsin Avenue, Room #001, Milwaukee, Wisconsin 53202.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 USC 2252 and 2252A, including:
 - a. Records containing child pornography or pertaining to the production, distribution, receipt, or possession of child pornography;
 - b. Records or information, photographs, videos, notes, documents, or correspondence, in any format or medium, concerning communications about child pornography or sexual activity with or sexual interest in minors;
2. All names, aliases, and numbers stored in the Device, including numbers associated with the Device, relating to the identities of those engaged in the production, possession, receipt, or distribution of child pornography.
3. Images or visual depictions of child pornography.
4. Records and information containing child erotica, including texts, images, and visual depictions of child erotica.
5. Any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to the violations.
6. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted by use of the computer or by other means for the purpose of committing the violations.
7. The list of all telephone calls made or received located in the memory of the Devices that provides information regarding the identities of and the methods and means of operation and communication by those engaged in the possession, receipt, or distribution of child pornography.
8. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning membership in online groups, clubs, or services that provide or make accessible child pornography.

9. Any and all information, records, documents, invoices, and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to the violations.

10. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.